AN ENUMERATION OF THE SETS OF NON-INTERFERING ARITHMETIC PROGRESSIONS WITH SPECIFIED PERIODS

By

EDWARD ALLEN FAY

A DISSERTATION PRESENTED TO THE GRADUATE COUNCIL OF
THE UNIVERSITY OF FLORIDA
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA
June, 1962

ACKNOWLEDGMENTS

The author wishes to acknowledge his indebtedness and to express his sincere appreciation to Dr. J. E. Maxfield, Head of the Department of Mathematics and Chairman of the Supervisory Committee, for his unfailing assistance and encouragement. In 1959, when Dr. Maxfield was still at the United States Naval Ordnance Test Station, China Lake, California, his correct conjecture of the result for $n = 3$ first aroused the author's interest in the problem. To Mr. R. S. Gardner, Dr. R. B. Leipnik, Dr. M. W. Maxfield, and Dr. H. Minc, who read the manuscript at various stages of its development, the author is indebted for many helpful suggestions. He wishes to thank Dr. W. O. Ash, Dr. R. G. Blake, Dr. E. H. Hadlock, and Dr. Minc for their help and encouragement as members of the Supervisory Committee. Finally, the author takes pleasure in acknowledging that his study at the University of Florida was made possible through the grant of an educational fellowship from his employer, the United States Naval Ordnance Test Station.

TABLE OF CONTENTS

Page

ACKNOWLEDGMENTS ii

NOTATION iv

Section

1. STATEMENT OF THE PROBLEM 1
2. OUTLINE OF THE ARGUMENT 3
3. THE CHINESE REMAINDER THEOREM AND ITS GENERALIZATION BY GAUSS 5
4. APPLICATION OF THE PRINCIPLE OF INCLUSION AND EXCLUSION 11
5. APPLICATION OF GROUP THEORY 13
6. GRAPH-THEORETIC CONSIDERATIONS, COMPLETING THE DERIVATION 17
7. ILLUSTRATIVE COMPUTATION 27
8. EXPLICIT FORMULAS FOR $F_n(\underline{b})$ 30
9. NUMERICAL EXAMPLE 33
10. A REDUCTION PRINCIPLE 35

REFERENCES 37

BIOGRAPHICAL SKETCH 38

NOTATION

(All lower-case symbols
precede all capital-letter symbols)

a	An arbitrary integer (Lemma 1 only); an arbitrary property (Lemma 3 only)
$\underline{a}$	A variable ordered n-tuple of integers a_i
$\underline{a}$ R A	The member $\underline{a}$ of G_o bears the relation R to the subset A of B
a_i	The ith component of $\underline{a}$, satisfying $0 \leq a_i < b_i$; also (Section 3 only) the right-hand side of the ith congruence of the system (2)
$\underline{a}^o$	A member of G_{k-1} whose existence is proved in Theorem 9
a_i^o	The ith component of $\underline{a}^o$
$\underline{a}^j$	The jth of several members of G_o discussed in the same context
a_i^j	The ith component of $\underline{a}^j$
$\underline{a}^1 + \underline{a}^2$	Sum of $\underline{a}^1$ and $\underline{a}^2$ under the operation of addition defined on G_o
b	An arbitrary integer (Lemma 1 only); an arbitrary property (Lemma 3 only); the common value of $b_1 = b_2 = \ldots = b_n$ (Theorem 12 only)

$\underline{b}$	A fixed ordered n-tuple of positive integers b_i
b_i	The ith component of $\underline{b}$
c	An arbitrary property
d	The greatest common divisor (a, b) (Lemma 1 only)
d_r	The greatest common divisor $d(C_r) = d(i_k ce \ldots zj_k) = (b_{i_k}, b_c, b_e, \ldots , b_z, b_{j_k})$
$d(ij \ldots z)$	The greatest common divisor $(b_i, b_j, \ldots , b_z)$, where $\{b_i, b_j, \ldots , b_z\}$ is a subset of the set of components of $\underline{b}$
$d(C)$	The greatest common divisor $d(ice \ldots zj) = (b_i, b_c, b_e, \ldots , b_z, b_j)$, where C is the path $Q_iQ_cQ_e \ldots Q_zQ_j$
f_k	A positive integer, defined to be 1 if $q = 0$ and to be the least common multiple $[d_1, d_2, \ldots , d_q]$ if $q > 0$
g	The order of the group G
g_k	A positive integer, defined to be $d(i_kj_k)$ if $G_{k-1} = G_k$, and otherwise to be the minimum positive residue of $a_{i_k} - a_{j_k}$ modulo $d(i_kj_k)$ as $\underline{a}$ varies over G_{k-1}
h	The index of the subgroup K in the group G
h_k	The index of G_k in G_{k-1}

$(i; j)$	An interference; $\underline{a}$ is said to exhibit the interference $(i; j)$ if and only if $i \neq j$ and the equation $a_i + hb_i = a_j + kb_j$ possesses a solution in integers h, k
k	The order of the subgroup K (Lemma 6 only); also (Theorem 6 *et seq.*) an integer satisfying $1 \leq k \leq m$
m	The number of interferences in a specified set of interferences $(i_1; j_1), (i_2; j_2), \ldots, (i_m; j_m)$; also (Section 3 only) the least common multiple $[m_1, m_2, \ldots, m_n]$ (specializing to $m_1 m_2 \ldots m_n$ in Theorem 1); also (Theorem 10 only) an integer satisfying $1 \leq m \leq n$
m_i	The modulus of the ith congruence of the system (2)
$m(\underline{a})$	The number of interferences $(i; j)$, with $i < j$, exhibited by $\underline{a}$
n	A fixed positive integer, the number of components of $\underline{a}$ and of $\underline{b}$; also (Section 3 only), the number of congruences in the system (2)
q	The number of paths in H connecting Q_{i_k} and Q_{j_k}
q_i	The number of paths in H connecting Q_t and Q_i
t	An integer satisfying $2 \leq t \leq n$

u	The sum $q_1 + q_2 + \cdots + q_{t-1}$
x	The unknown in the system (2) of simultaneous congruences
A	A subset of B; in the proof of Theorem 9 the particular subset $\{Q_{i_k}, Q_{j_k}\}$; also (Lemma 7 only) a subgroup
A_{t-1}	A subset of B of the specific form $\{Q_1, Q_2, \ldots, Q_{t-1}\}$
B	The set of points of the linear graph H; also (Lemma 7 only) a subgroup
C	A path $Q_iQ_cQ_e \ldots Q_zQ_j$ in the linear graph H; also (Lemma 7 only) a subgroup
C_r	The rth path $C_r = Q_{i_k}Q_cQ_e \ldots Q_zQ_{j_k}$ of the q paths connecting Q_{i_k} and Q_{j_k}
C_{ij}	A path constructed in the proof of Theorem 8
C_{it}	The path C_{ti} with direction reversed
C_{ti}	A directed path from Q_t to Q_i
C^p_{ti}	The pth of the q_i paths connecting Q_t and Q_i
C_{tj}	A directed path from Q_t to Q_j
C^r_{tj}	The rth of the q_j paths connecting Q_t and Q_j
$F_n(\underline{b})$	The number of members of G_0 which belong to the subset T; thus, the number of members of G_0 which exhibit no interferences
G	A finite abelian group
G_0	The set of all possible choices for $\underline{a}$

G_k	The subgroup made up of members *a* of G_o that exhibit at least the interferences $(i_1;\ j_1),\ (i_2;\ j_2),\ \dots,\ (i_k;\ j_k)$
H	A specific linear graph with n points Q_i and k - 1 links Q_iQ_j (*q. v.*)
J	The subgroup of G_o whose members exhibit all possible interferences
K	In general (Lemmas 5 and 6), a subgroup of a finite abelian group G; in particular (Theorem 5), a subgroup of G_o whose members exhibit at least the specified interference (i; j)
N	The number of objects in some set of objects
N(a)	The number of objects having property a
N(ab)	The number of objects having properties a and b
N(a'b'c' ...)	The number of objects having none of the properties a, b, c, ...
$N((i_1;\ j_1)(i_2;\ j_2)\ \dots\ (i_m;\ j_m))$	The number of members *a* of G_o that exhibit at least the interferences $(i_1;\ j_1),\ (i_2;\ j_2),\ \dots,\ (i_m;\ j_m)$
$P_i(a_i)$	The arithmetic progression $\{a_i + hb_i\text{: } h = 0, 1, 2, \dots\}$, with period b_i and initial value a_i

Q_i	The ith point of a linear graph, in particular of the graph H
Q_m	The first point of C_{it} that is also a point of C_{tj}
Q_iQ_j	The link joining points Q_i and Q_j of a linear graph; Q_iQ_j is a link of H if and only if (i; j) is one of the interferences $(i_1; j_1), (i_2; j_2), \ldots , (i_{k-1}; j_{k-1})$
$Q_1Q_2 \cdots Q_k$	The path which is the collection of links $Q_1Q_2, Q_2Q_3, \cdots , Q_{k-1}Q_k$
R	A certain relation with domain G_o and range the class of all subsets of B
R_i	A coset relative to K
$S(\underline{a})$	The ordered n-tuple $\{P_1(a_1), P_2(a_2), \ldots , P_n(a_n)\}$ of arithmetic progressions
T	The subset of G_o consisting of those members $\underline{a}$ for which $m(\underline{a}) = 0$; thus, the subset whose members exhibit no interferences
(, , ... ,)	Greatest common divisor
[, , ... ,]	Least common multiple
{ , , ... , }	A pair, triple, ... , or n-tuple, whether ordered or not

SECTION 1

STATEMENT OF THE PROBLEM

Let n be a fixed positive integer, let $\underline{b} = \{b_1, b_2, \ldots, b_n\}$ be a fixed ordered n-tuple of positive integers, and let $\underline{a} = \{a_1, a_2, \ldots, a_n\}$ be a variable ordered n-tuple of integers such that $0 \leq a_i < b_i$, $i = 1, 2, \ldots, n$. Let G_0 be the set of all $b_1 b_2 \ldots b_n$ possible choices for $\underline{a}$. With each component a_i of each member $\underline{a}$ of G_0 associate the infinite sequence $P_i(a_i) = \{a_i + hb_i : h = 0, 1, 2, \ldots\}$.

Definition. $P_i(a_i)$ is called an arithmetic progression with period b_i and initial value a_i.

With each $\underline{a}$ in G_0 associate the ordered n-tuple $S(\underline{a}) = \{P_1(a_1), P_2(a_2), \ldots, P_n(a_n)\}$ of arithmetic progressions. Let $\underline{a}$ be any member of G_0 and let $\{P_i(a_i), P_j(a_j)\}$, $i \neq j$, be any pair of distinct components of $S(\underline{a})$.

Definition. If the equation

$$a_i + hb_i = a_j + kb_j \tag{1}$$

possesses a solution in integers $\{h, k\}$, the pair $\{P_i(a_i), P_j(a_j)\}$ of arithmetic progressions is said to interfere, and the member $\underline{a}$ of G_0 is said to exhibit the interference (i; j).

It is an immediate consequence of the definition that a member a of G_0 exhibits both or neither of the interferences $(i; j)$ and $(j; i)$. Thus, in counting the number $m(\underline{a})$ of interferences exhibited by a, we may restrict the count to interferences $(i; j)$ with $i < j$, and it is possible a priori that $m(\underline{a})$ may assume any integer value in the interval $0 \leq m(\underline{a}) \leq n(n - 1)/2$. Let T be the subset of G_0 consisting of those members a of G_0 such that $m(\underline{a}) = 0$, and let $F_n(\underline{b})$ be the number of members of G_0 which belong to the subset T. The problem undertaken is to develop a rule for evaluating $F_n(\underline{b})$.

SECTION 2

OUTLINE OF THE ARGUMENT

In Section 3 the Chinese remainder theorem and its generalization by Gauss are stated and proved; the latter theorem will be our principal number-theoretic tool. The next three sections describe the evaluation of $F_n(\underline{b})$ in progressively finer detail. In Section 4 the principle of inclusion and exclusion is applied to express $F_n(\underline{b})$ in terms of the sizes of subsets of G_0 whose members exhibit specified sets of interferences, since it turns out that these subsets are simpler in structure than T. In fact, in Section 5 it is shown that, under a suitably defined operation, G_0 is an abelian group and these subsets are subgroups, some contained within others; the problem is thus reduced to the evaluation of the index h_k of a subgroup G_k in a group G_{k-1} containing it. In Section 6, which is the heart of the argument, h_k is evaluated by means of a detailed comparison of the constraints imposed on $\underline{a}$ when a set of k interferences, or a subset consisting of k - 1 of them, is specified; it is convenient and natural to express this argument in the language of linear graph theory.

In Section 7 an example illustrates the results of the two preceding sections. In Section 8 explicit formulas are displayed for $F_n(\underline{b})$, $n = 1, 2, 3, 4$. In Section 9 the formulas are illustrated by a numerical example. In Section 10 a reduction principle is noted which permits an abbreviated calculation in some cases.

SECTION 3

THE CHINESE REMAINDER THEOREM AND ITS GENERALIZATION BY GAUSS

Dickson [1, pp. 57-64] traces the history of the problem of solving a system

(2) $x \equiv a_1 \bmod m_1,\ x \equiv a_2 \bmod m_2,\ \ldots\ ,\ x \equiv a_n \bmod m_n$

of simultaneous congruences in one unknown with different moduli. Rules for solving (2) when a solution exists, in more or less special cases, are traced as far back as the Chinese scholar Sun-Tsŭ, about the first century A. D. [1, pp. 57-58]. Theorem 1 below, known as the Chinese remainder theorem, states that a solution always exists (without restriction on the a_i) if the m_i are relatively prime in pairs. The special cases treated by Sun-Tsŭ and by many of the later writers satisfy this condition.

The more difficult problem of formulating necessary and sufficient conditions (on the a_i and the m_i jointly) in order that the system (2) be consistent was apparently not solved before the eighteenth century. Theorem 2 below states such conditions in what is probably the most compact form possible. We prove Theorem 2 following the outline by Dickson

[1, p. 63] of a proof (1801) by Gauss, but Dickson's account does not clearly attribute priority to Gauss; the same necessary and sufficient conditions may have been known to Saunderson (1740) or to Lagrange (1767) [1, pp. 61-63].

Following the usual conventions, we denote the greatest common divisor and least common multiple of a set $\{c_1, c_2, \ldots , c_k\}$ of integers by $(c_1, c_2, \ldots , c_k)$ and $[c_1, c_2, \ldots , c_k]$ respectively. We agree that $(0, 0) = 0$, and therefore in all cases $(0, c) = (c, 0) = |c|$. In later sections, when the set of integers is in particular a subset of the set of components of $\underline{b}$, we shall further abbreviate $(b_i, b_j, \ldots , b_z)$ as $d(ij \ldots z)$.

Lemma 1. If $d = (a, b)$, there exist integers p and s such that $d = pa + sb$.

Proof: If $a = b$, $d = |a|$; if either a or b is 0, their greatest common divisor is the absolute value of the other; thus, in either of these cases, the conclusion is immediate. If the lemma holds for positive integers a and b, it holds for all integers, because a change of sign in a or b can be accommodated by a corresponding change in p or s. Therefore we assume without loss of generality that $a > b > 0$. We take as known Euclid's division algorithm, according to which it is possible to write a finite chain of equations

$$\begin{aligned}
a &= bq + r, & 0 &< r < b,\\
b &= rq_1 + r_1, & 0 &< r_1 < r,\\
r &= r_1q_2 + r_2, & 0 &< r_2 < r_1,\\
&\dots & &\dots\\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1}, & 0 &< r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1}q_k + r_k, & 0 &< r_k < r_{k-1},\\
r_{k-1} &= r_kq_{k+1},
\end{aligned} \tag{3}$$

such that the last positive remainder r_k equals d.

Ignoring the last equation in the chain (3), we may eliminate r_{k-1} from the two preceding equations and express r_k as a linear combination, with integer coefficients, of r_{k-3} and r_{k-2}. Then we may eliminate r_{k-2} and express r_k as a linear combination of r_{k-4} and r_{k-3}, and so on. In the final step we may eliminate r and obtain an equation of the form $d = r_k = pa + sb$, as required.

Lemma 2. If $(m_1, m_2) = 1$, the two congruences

$$x \equiv 0 \bmod m_1,\ x \equiv 1 \bmod m_2$$

have a common solution.

Proof: By Lemma 1, there exist integers p and s such that $pm_1 + sm_2 = 1$. Then $x = pm_1$ satisfies

$$x \equiv 0 \bmod m_1,\ x \equiv 1 \bmod m_2,$$

as required.

Theorem 1 (Chinese remainder theorem). If $(m_i, m_j) = 1$ for every pair $\{i, j\}$, $i \neq j$, then

$$x \equiv a_1 \bmod m_1,\ x \equiv a_2 \bmod m_2,\ \dots,\ x \equiv a_n \bmod m_n \tag{2}$$

has a unique solution modulo $m = m_1m_2 \dots m_n$.

Proof: Since m_i is relatively prime to each m_j, $j \neq i$, m_i is relatively prime to their product $m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_n = m/m_i$. Then, for each i, $i = 1, 2, \ldots, n$, by Lemma 2 the two congruences

$$x \equiv 0 \bmod m/m_i,\quad x \equiv 1 \bmod m_i$$

have a common solution; call it x_i, and let $x = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$.

Now for each $j \neq i$, m_i divides m/m_j, which in turn divides x_j. Then $x_j \equiv 0 \bmod m_i$, whence $x \equiv a_i x_i \equiv a_i \bmod m_i$, which is the ith of the congruences (2). Then x satisfies (2). Then any other integer y is a solution if and only if $y - x$ is divisible by each of the m_i, hence by their product m. Thus (2) has a unique solution modulo m, completing the proof.

Theorem 2 (Gauss). A necessary and sufficient condition in order that

(2) $x \equiv a_1 \bmod m_1,\ x \equiv a_2 \bmod m_2,\ \ldots,\ x \equiv a_n \bmod m_n$

have a solution is that (m_i, m_j) divide $a_i - a_j$ for every pair $\{i, j\}$, $i \neq j$. There is then just one solution in the interval $0 \leq x < m$, where $m = [m_1, m_2, \ldots, m_n]$.

Proof: Let $p_1, p_2, \ldots, p_q$ be all the distinct primes that occur in the prime-power factorization of m, and let $m_i = p_1^{e_{i1}} p_2^{e_{i2}} \ldots p_q^{e_{iq}}$, $i = 1, 2, \ldots, n$, where some exponents may be zero. Then we notice first that the system (2) of n congruences is equivalent to the system

(4) $x \equiv a_i \bmod p_k^{e_{ik}}$; $i = 1, 2, \ldots, n$; $k = 1, 2, \ldots, q$

of nq congruences, for $x - a_i$ is divisible by m_i if and only if it is divisible by each prime-power factor $p_k^{e_{ik}}$ of m_i.

Now suppose that x satisfies (2), or, equivalently, (4). Suppose that, for some particular i, j, and k, $e_{ik} \leq e_{jk}$. Then $p_k^{e_{ik}}$ divides $p_k^{e_{jk}}$, which in turn divides $x - a_j$. Then $a_i \equiv x \equiv a_j \bmod p_k^{e_{ik}}$. Similarly we conclude that

$$a_i \equiv a_j \bmod p_k^{\min\{e_{ik}, e_{jk}\}}$$

for $k = 1, 2, \ldots, q$. Then $a_i - a_j$ is divisible by each of these relatively prime moduli, hence by their product. But their product is (m_i, m_j), so we have that (m_i, m_j) divides $a_i - a_j$. Therefore, since the pair $\{i, j\}$, $i \neq j$, is arbitrary, the conditions hold.

Suppose conversely that the conditions are satisfied, and let $m = p_1^{f_1} p_2^{f_2} \ldots p_q^{f_q}$. Then each $p_k^{f_k}$ occurs in the prime-power factorization of one or more of the m_i; if $p_k^{f_k}$ occurs in the prime-power factorization of more than one of the m_i, choose one of the latter arbitrarily; let $c_k = a_i$ for the i such that $p_k^{f_k}$ occurs in the prime-power factorization of m_i. Since $(p_k^{f_k}, p_r^{f_r}) = 1$ for every pair $\{k, r\}$, $k \neq r$, the system of congruences

$x \equiv c_1 \bmod p_1^{f_1}$, $x \equiv c_2 \bmod p_2^{f_2}$, $\ldots$, $x \equiv c_q \bmod p_q^{f_q}$

has a unique solution modulo m, by Theorem 1. Call this solution x.

Now fix j and k, and let i be the subscript such that $p_k^{f_k}$ occurs in the prime-power factorization of m_i. Then $e_{jk} \leq f_k = e_{ik}$, and $p_k^{e_{jk}}$ divides $p_k^{f_k}$, which in turn divides $x - c_k = x - a_i$. Also $p_k^{e_{jk}}$ divides (m_i, m_j), which divides $a_i - a_j$ by hypothesis. Then $x \equiv a_i \equiv a_j \bmod p_k^{e_{jk}}$, and we have established a typical one of the nq congruences (4). Therefore, since j and k are arbitrary, x satisfies the system (4), and hence, equivalently, the system (2). Since we have already noted that x is unique modulo m, this completes the proof.

SECTION 4

APPLICATION OF THE PRINCIPLE OF INCLUSION AND EXCLUSION

We quote without proof the principle of inclusion and exclusion in the form stated by Riordan [3, p. 51].

Lemma 3 (Principle of inclusion and exclusion). If of N objects, N(a) have property a, N(b) property b, ... , N(ab) both a and b, ... , N(abc) a, b, and c, and so on, then the number N(a'b'c' ...) with none of these properties is given by

$$\begin{aligned} N(a'b'c' \ldots) = N &- N(a) - N(b) - \ldots \\ &+ N(ab) + N(ac) + \ldots \\ &- N(abc) - \ldots \\ &+ \ldots . \end{aligned}$$

Restricting our attention to interferences $(i;\ j)$ with $i < j$, let $N((i_1;\ j_1)(i_2;\ j_2) \ldots (i_m;\ j_m))$ be the number of members $\underline{a}$ of G_o that exhibit at least the interferences $(i_1;\ j_1)$, $(i_2;\ j_2)$, ... , $(i_m;\ j_m)$ with respect to the fixed n-tuple $\underline{b} = \{b_1, b_2, \ldots , b_n\}$, where $1 \leq m \leq n(n - 1)/2$.

Theorem 3.

$$
\begin{aligned}
F_n(\underline{b}) = b_1 b_2 \dots b_n &- N((1;2)) - N((1;3)) - \dots - N((n-1;n)) \\
&+ N((1;2)(1;3)) + N((1;2)(1;4)) + \dots + N((n-2;n)(n-1;n)) \\
&- \dots \\
&+ (-1)^{n(n-1)/2} N((1;2)(1;3)\dots(n-1;n)).
\end{aligned} \tag{5}
$$

Proof: Theorem 3 is an immediate application of Lemma 3. The objects to be classified are the $b_1 b_2 \dots b_n$ members $\underline{a}$ of G_o, and the properties a, b, c, ... are the $n(n - 1)/2$ possible interferences $(i;\ j)$, $i < j$.

SECTION 5

APPLICATION OF GROUP THEORY

We adapt from Ledermann [2], without proof, four lemmas from the elementary theory of finite abelian groups.

Lemma 4 [2, p. 9, Theorem 1]. A finite set of elements for which a law of composition ("addition") is defined forms an abelian group if

(a) the set is closed with respect to addition;

(b) the associative law is satisfied;

(c) the commutative law is satisfied;

(d) the equation $a + x = b + x$ implies that $a = b$.

Thus Lemma 4 states that, in the case of a finite set of elements, the listed conditions imply the presence in the set of an identity element ("zero") and of an additive inverse for each element of the set.

Lemma 5 [2, p. 31, Theorem 1]. A non-empty subset K of a finite group under addition is a subgroup if and only if it is closed with respect to addition.

Definition. The number of elements in a finite group is called the order of the group.

Lemma 6 (Lagrange's theorem) [2, pp. 34-35, Theorem 3]. If K is a subgroup of a finite abelian group G, where the orders of these groups are k and g respectively, then k divides g, i. e. $g = hk$ for some integer h. The integer h is called the index of K in G. There exists a set of h elements $r_1, r_2, \ldots, r_h$ in G such that G is the union of h disjoint subsets $R_i = \{x + r_i : x \in K\}$, $i = 1, 2, \ldots, h$, called cosets relative to K and each with k members.

Lemma 7 [2, p. 41, Theorem 6]. The intersection of subgroups A, B, C, ... is a subgroup of each of the groups A, B, C, ...

Now we are ready to start applying these group-theoretic concepts to the problem of evaluating $F_n(\underline{b})$.

Definition. Let $\underline{a}^1 = \{a_1^1, a_2^1, \ldots, a_n^1\}$ and $\underline{a}^2 = \{a_1^2, a_2^2, \ldots, a_n^2\}$ be any two members of G_o. Then their sum $\underline{a}^1 + \underline{a}^2$ is defined as the unique ordered n-tuple $\underline{a}^3 = \{a_1^3, a_2^3, \ldots, a_n^3\}$ such that $a_i^3 \equiv a_i^1 + a_i^2 \mod b_i$, $0 \leq a_i^3 < b_i$; $i = 1, 2, \ldots, n$.

Theorem 4. G_o is a finite abelian group under the operation of addition just defined.

Proof: Since addition modulo b_i is uniquely defined and since $0 \leq a_i^3 < b_i$ for each i, $\underline{a}^3$ belongs to G_o when $\underline{a}^1$ and $\underline{a}^2$ do; then G_o is closed with respect to addition. The associative and commutative laws hold in G_o because they hold component by component. Since identity of two members of G_o implies identity component by component, and since subtraction modulo b_i is uniquely defined, the cancellation law holds in G_0. Since G_0 is a finite set, all the requirements of Lemma 4 are satisfied.

Theorem 5. The subset K made up of members $\underline{a}$ of G_0 that exhibit at least the single specified interference (i; j) is a subgroup of G_0.

Proof: We note that the defining condition (1) for interference is equivalent to requiring the existence of an integer x satisfying simultaneously the congruences

$$x \equiv a_i \bmod b_i, \; x \equiv a_j \bmod b_j.$$

By Theorem 2, this condition is equivalent to the condition that $d(ij) = (b_i, b_j)$ divide $a_i - a_j$, i. e., is equivalent to the condition that $a_i \equiv a_j \bmod d(ij)$.

Let $\underline{a}^1$ and $\underline{a}^2$ be any two members of K, and let $\underline{a}^3 = \underline{a}^1 + \underline{a}^2$. Then

$$a_i^1 \equiv a_j^1 \bmod d(ij), \; a_i^2 \equiv a_j^2 \bmod d(ij),$$

whence

$$a_i^3 \equiv a_i^1 + a_i^2 \equiv a_j^1 + a_j^2 \equiv a_j^3 \bmod d(ij),$$

so that $\underline{a}^3$ belongs to K. Thus K is closed with respect to addition. Further, K is non-empty, for it has at least the member $\underline{0} = \{0, 0, \ldots, 0\}$. Then, by Lemma 5, K is a subgroup of G_0, q. e. d.

Now, in order to evaluate a term $N((i_1; j_1)(i_2; j_2) \ldots (i_m; j_m))$ appearing in (5), for each k, $1 \leq k \leq m$, let G_k be the subset made up of members $\underline{a}$ of G_0 that exhibit at least the interferences $(i_1; j_1), (i_2; j_2), \ldots, (i_k; j_k)$.

Theorem 6. For each k, $1 \leq k \leq m$, G_k is a subgroup of G_{k-1}.

Proof: We proceed by induction on k. G_1 is a subgroup of G_o by Theorem 5. Suppose that G_{k-1} is a subgroup of G_o and of G_{k-2}. Then G_k is the intersection of G_o, of G_{k-1}, and of the subset made up of members a of G_o that exhibit at least the interference $(i_k;\ j_k)$, and the latter set is a subgroup of G_o by Theorem 5; therefore G_k is a subgroup of G_o and of G_{k-1}, by Lemma 7, completing the induction.

Now appealing to Lemma 6 and letting h_k be the index of G_k in G_{k-1} for each k, $1 \leq k \leq m$, we infer

Theorem 7.

(6) $N((i_1;j_1)(i_2;j_2)\ldots(i_m;j_m)) = b_1b_2\ldots b_n\ /\ h_1h_2\ldots h_m$.

Proof: The order of G_o is $b_1b_2 \ldots b_n$. The equation $g = hk$ in Lemma 6, relating the order g of a finite group G, the order k of a subgroup K, and the index h of K in G, may be rewritten $k = g/h$. Then the order of G_1 is $b_1b_2 \ldots b_n/h_1$, the order of G_2 is $\overline{b_1b_2 \ldots b_n/h_1}/h_2 = b_1b_2 \ldots b_n/h_1h_2$, and so on. Finally, the order of G_m is given by the right-hand side of (6). But it is also given by the left-hand side of (6). This completes the proof.

SECTION 6

GRAPH-THEORETIC CONSIDERATIONS, COMPLETING THE DERIVATION

In Theorems 6 and 7 we restricted our attention to the evaluation of a single typical term (6) appearing in (5). In the present section we restrict our attention even more narrowly, to the evaluation of a single typical index h_k appearing in (6). Thus the value of k and the interferences $(i_1; j_1)$, $(i_2; j_2)$, ... , $(i_k; j_k)$ will be considered fixed throughout the present section.

We can see in advance that the index h_k of the subgroup G_k in G_{k-1} must somehow be a measure of comparison between the system of constraints imposed on a by the interferences $(i_1; j_1)$, $(i_2; j_2)$, ... , $(i_{k-1}; j_{k-1})$ and the system of constraints imposed on a by these k - 1 interferences together with $(i_k; j_k)$. It is not hard to guess what may happen in extreme cases; if $(i_1; j_1)$, $(i_2; j_2)$, ... , $(i_{k-1}; j_{k-1})$ already constrain a so severely that $a_{i_k} - a_{j_k} \equiv 0 \bmod d(i_k j_k)$ for all a in G_{k-1}, then $G_{k-1} = G_k$ and $h_k = 1$; at the other extreme, if $a_{i_k} - a_{j_k}$ varies through all residue classes modulo $d(i_k j_k)$ as a varies over G_{k-1}, then (as we might expect) these residue classes can be put into correspondence with cosets relative to G_k, and $h_k = d(i_k j_k)$.

A general expression for h_k is eventually given in Theorem 9, but a substantial amount of preparation is required before Theorem 9 can be proved, or even stated. We must first introduce and apply several concepts (but no theorems) from the theory of linear graphs. We quote from Riordan [3, p. 109] the definitions we shall use.

Definitions. A linear graph is a collection of points, and a collection of links or pairs of points which describes the connections of points; a collection of n discrete points (without connecting links) is a graph and, at the other extreme, a collection of n points, each pair of which is joined by a link [so that there are $n(n - 1)/2$ links in total], is a graph, the complete graph. At most one link may join two points, and the graph has no links joining points to themselves. A cycle of a graph is a collection of links of the form Q_1Q_2, Q_2Q_3, ... , $Q_{k-1}Q_1$, where Q_iQ_j designates the link joining points Q_i and Q_j, and Q_1, Q_2, ... , Q_{k-1} are distinct points. A path is a collection of links of the form Q_1Q_2, Q_2Q_3, ... , $Q_{k-1}Q_k$, with all points Q_1, Q_2, ... , Q_k distinct; then the path is said to connect the points Q_1 and Q_k; we shall abbreviate the notation slightly, and call this path $Q_1Q_2 \dots Q_k$.

Now let us construct a linear graph H to serve as a model for the system of constraints imposed on a by the k - 1 interferences $(i_1; j_1)$, $(i_2; j_2)$, ... , $(i_{k-1}; j_{k-1})$. Let H have n points; call the set of points of H $B = \{Q_i: i = 1, 2, \ldots, n\}$, and let us put B into one-to-one correspondence with the set of n components of the fixed n-tuple b, and simultaneously into one-to-one correspondence with the set of n components of the variable n-tuple a, by associating Q_i with b_i and with a_i for each i, $i = 1, 2, \ldots, n$. In conformity with this correspondence, let H have k - 1 links, chosen so that Q_iQ_j is a link of H if and only if (i; j) is one of the k - 1 interferences $(i_1; j_1)$, $(i_2; j_2)$, ... , $(i_{k-1}; j_{k-1})$. We emphasize that the linear graph H will be considered fixed throughout the present section. Two points Q_i and Q_j will be said to be connected by a path $C = Q_iQ_cQ_e \ldots Q_zQ_j$ if Q_i, Q_c, Q_e, ... , Q_z, Q_j are distinct points (that is, if C is free of cycles), and if Q_iQ_c, Q_cQ_e, ... , Q_zQ_j are links chosen from among the k - 1 links of H. If Q_i and Q_j are connected by such a path C, let $d(C) = d(ice \ldots zj) = (b_i, b_c, b_e, \ldots, b_z, b_j)$, where b_i, b_c, b_e, ... , b_z, b_j are the components of b corresponding respectively to the points Q_i, Q_c, Q_e, ... , Q_z, Q_j of B.

Now we define a relation R with domain G_0 and with range the class of all subsets of B.

Definition. A member $\underline{a}$ of G_0 will be said to be R-related to a subset A of B, in symbols $\underline{a}$ R A, if and only if, for every pair $\{Q_i, Q_j\}$ of distinct members of A, and for every path C connecting Q_i and Q_j (C not confined to A, but the links of C confined to those of H), $a_i \equiv a_j \bmod d(C)$, where a_i and a_j correspond respectively to Q_i and Q_j under the correspondence between components and points.

If $A = \{Q_i, Q_j, \ldots, Q_z\}$ is a proper subset of B, we notice that the truth or falsity of $\underline{a}$ R A is determined as soon as numerical values of the components $a_i, a_j, \ldots, a_z$ of $\underline{a}$ are specified; that is, if $\underline{a}^1$ and $\underline{a}^2$ are two members of G_0 such that $a_i^1 = a_i^2, a_j^1 = a_j^2, \ldots, a_z^1 = a_z^2$, then the statements $\underline{a}^1$ R A and $\underline{a}^2$ R A are both true or both false.

Theorem 8. Let $A = \{Q_i, Q_j, \ldots, Q_z\}$ be a non-empty proper subset of B. If numerical values of $a_i, a_j, \ldots, a_z$ have been chosen so that $\underline{a}$ R A, then numerical values for the remaining components of $\underline{a}$ can be chosen so that $\underline{a}$ R B.

Proof: In order to simplify notation, we shall prove the theorem for a subset A of the specific form $A_{t-1} = \{Q_1, Q_2, \ldots, Q_{t-1}\}$, where $2 \leq t \leq n$. This restriction involves no loss of generality, because any non-empty proper subset A of B can be brought into the form A_{t-1} for some t by an appropriate relabelling of indices; it is understood that, in order to preserve the correspondence between components and points, the same relabelling is applied simultaneously to the components of a̲ and of b̲ and to the indices appearing in the symbols (i; j) defining the links of H. Thus the relabelling is purely a matter of notational convenience; in particular, we are still dealing with the same fixed set of k - 1 interferences, and with the same fixed linear graph H.

We notice further that the truth of the theorem will follow if, for arbitrary t, $2 \leq t \leq n$, we demonstrate the possibility of a single inductive step; that is, if we show that, when numerical values of $a_1, a_2, \ldots, a_{t-1}$ have been chosen so that a̲ R A_{t-1}, then a numerical value for a_t can be chosen so that a̲ R A_t.

Thus fix t and suppose that numerical values of $a_1, a_2, \ldots, a_{t-1}$ have been chosen so that a̲ R A_{t-1}. Let the number of paths in H connecting Q_t and Q_i be q_i, $i = 1, 2, \ldots, t-1$. Then a̲ R A_t if a_t can be chosen to satisfy the following system of $u = q_1 + q_2 + \ldots + q_{t-1}$ congruences:

(7) $a_t \equiv a_i \bmod d(C^p_{ti})$; $p=1,2,\ldots,q_i$; $i=1,2,\ldots,t-1$;

where C^p_{ti} is the pth of the q_i paths connecting Q_t and Q_i. If $u = 0$, then no restriction is imposed on a_t, and it suffices to take $a_t = 0$. If $u = 1$, it suffices to choose a_t to satisfy a single congruence (7); this can be done because $d(C^p_{ti}) \leq b_t$. If $u \geq 2$, then, by Theorem 2, a_t can be chosen to satisfy the system (7) provided $a_1, a_2, \ldots, a_{t-1}$ satisfy the following system of congruences:

$$\begin{aligned} &a_i \equiv a_j \bmod (d(C^p_{ti}), d(C^r_{tj})); \\ (8)\qquad &p = 1,2,\ldots,q_i;\ r = 1,2,\ldots,q_j;\ i,j = 1,2,\ldots,t-1. \end{aligned}$$

Some of the congruences appearing in (8) may be trivial; let us dispose of them first. If $q_i \geq 2$, then there exist pairs of congruences in (7) both of the form $a_t \equiv a_i$, though with possibly different moduli, and the congruence of the system (8) corresponding to such a pair is of the form $a_i \equiv a_i$, which holds to any modulus.

Having disposed of the trivial cases, let us seek to establish an arbitrarily chosen congruence of the system (8), with $i \neq j$. Having chosen one of the congruences, we may omit the superscripts p and r in the symbols for the two paths involved. Let us now regard C_{ti} as a directed path from Q_t to Q_i and C_{tj} as a directed path from Q_t to Q_j, and indicate a reversal of direction by a transposition of subscripts. We can find in H a path C_{ij} connecting Q_i to Q_j as follows. Let Q_m be the first point of C_{it} that is also a point of C_{tj}; there exists at least one common point, for Q_t is one. Let C_{ij} be the path described by following C_{it} from Q_i to Q_m, then following C_{tj} from Q_m to Q_j (counting Q_m itself only once, of course). Then, because of the choice of Q_m, C_{ij} satisfies the defining conditions for a path; it is free of cycles because C_{it} and C_{tj} are, and because Q_m is the first point of C_{it} that is also a point of C_{tj}; also, since every link of C_{ij} is either a link of C_{it} or of C_{tj}, the links of C_{ij} are chosen from among those of H.

Now the chosen congruence of the system (8) asserts that $a_i - a_j$ is divisible by $(d(C_{ti}), d(C_{tj}))$. But this congruence does, in fact, hold, for the hypothesis that $\underline{a}$ R A_{t-1} assures that $a_i - a_j$ is divisible by $d(C_{ij})$; then $d(C_{ij})$, in turn, is divisible by $(d(C_{ti}), d(C_{tj}))$ since the b_p appearing in $d(C_{ij})$ are a subset of those appearing in $(d(C_{ti}), d(C_{tj}))$.

Thus the whole system of congruences (8) holds, so the congruences of the system (7) have a common solution a_t. Since each of the u moduli in the system (7) divides b_t, so does their least common multiple, and Theorem 2 then assures us that a_t can be chosen in the interval $0 \leq a_t < b_t$. This completes the proof of Theorem 8.

Now consider the interference $(i_k; j_k)$. Let the points Q_{i_k} and Q_{j_k} be connected (still in the fixed linear graph H having only k - 1 links) by exactly q paths $C_1, C_2, \ldots, C_q$. We shall define a positive integer f_k as follows. If $q = 0$, let $f_k = 1$.

If $q > 0$ and $C_r = Q_{i_k}Q_cQ_e \ldots Q_zQ_{j_k}$, let $d_r = d(C_r) = d(i_k ce \ldots z j_k) = (b_{i_k}, b_c, b_e, \ldots, b_z, b_{j_k})$, where b_{i_k}, b_c, b_e, ... , b_z, b_{j_k} correspond respectively to Q_{i_k}, Q_c, Q_e, ... , Q_z, Q_{j_k} under the correspondence between components and points, and let $f_k = [d_1, d_2, \ldots, d_q]$.

Theorem 9. The value of the index h_k of G_k in G_{k-1} is

$$h_k = d(i_k j_k)/f_k. \tag{9}$$

Proof: According to Lemma 6, the subgroup G_k induces a decomposition of G_{k-1} into h_k cosets of equal size. Since two members $\underline{a}^1$ and $\underline{a}^2$ of G_{k-1} belong to G_k if and only if

$$a^1_{i_k} - a^1_{j_k} \equiv a^2_{i_k} - a^2_{j_k} \equiv 0 \bmod d(i_k j_k),$$

it follows from the definition of a coset that two members $\underline{a}^3$ and $\underline{a}^4$ of G_{k-1} belong to the same coset relative to G_k if and only if

$$a^3_{i_k} - a^3_{j_k} \equiv a^4_{i_k} - a^4_{j_k} \bmod d(i_k j_k),$$

that is, if and only if $a^3_{i_k} - a^3_{j_k}$ and $a^4_{i_k} - a^4_{j_k}$ belong to the same residue class modulo $d(i_k j_k)$.

Among the residues of $a_{i_k} - a_{j_k}$ modulo $d(i_k j_k)$ for the various members $\underline{a}$ of G_{k-1}, there is some least positive residue g_k unless $a_{i_k} - a_{j_k} \equiv 0 \bmod d(i_k j_k)$ for all $\underline{a}$ in G_{k-1}, in which case $G_k = G_{k-1}$ and we take $g_k = d(i_k j_k)$. In either case, by the closure property of the group G_{k-1}, there is a coset corresponding to each of the residues

$0, g_k, 2g_k, \ldots, d(i_kj_k) - g_k$, and only to these, for the existence of a member $\underline{a}$ of G_{k-1} for which division of $a_{i_k} - a_{j_k}$ by g_k left a positive remainder would show that remainder to be a smaller residue than g_k, contradicting the definition of g_k. Therefore $h_k = d(i_kj_k)/g_k$.

We shall prove that the positive integer f_k defined just before the statement of the theorem divides $a_{i_k} - a_{j_k}$ for every $\underline{a}$ in G_{k-1}, and it will follow that f_k divides the least positive residue g_k. We shall prove also that $a^o_{i_k} - a^o_{j_k} \equiv f_k \bmod d(i_kj_k)$ for some $\underline{a}^o$ in G_{k-1}, and it will follow, as we have just seen, that f_k must be a multiple of the least positive residue g_k. From the mutual divisibility of the positive integers f_k and g_k it will then follow that $f_k = g_k$, and hence that (9) holds.

If $q = 0$, then $f_k = 1$, which divides $a_{i_k} - a_{j_k}$ for every $\underline{a}$ in G_{k-1}. If $q > 0$, then, along any path C_r, $a_{i_k} - a_{j_k}$ may be decomposed as
$$a_{i_k} - a_{j_k} = (a_{i_k} - a_c) + (a_c - a_e) + \ldots + (a_z - a_{j_k}),$$
and since, for $\underline{a}$ in G_{k-1}, each term $a_u - a_v$ in this sum is divisible by $d(uv)$, we have that $a_{i_k} - a_{j_k}$ is divisible by $(d(i_kc), d(ce), \ldots, d(zj_k)) = d_r$. Since $a_{i_k} - a_{j_k}$ is thus divisible by d_r for each path C_r, $a_{i_k} - a_{j_k}$ is divisible by the least common multiple of the d_r, namely f_k.

To construct $\underline{a}^o$, notice first that b_{i_k} is divisible by each d_r, hence by their least common multiple f_k (or by $f_k = 1$ if $q = 0$). Then $f_k \leq b_{i_k}$. Let $a^o_{i_k} = f_k$ if $f_k < b_{i_k}$, and let $a^o_{i_k} = 0$ if $f_k = b_{i_k}$; let $a^o_{j_k} = 0$. Then $a^o_{i_k} - a^o_{j_k} \equiv f_k \bmod d(i_k j_k)$ in either of the possible cases for f_k; if $f_k < b_{i_k}$, the congruence holds as an equality, and if $f_k = b_{i_k}$, the congruence holds because $a^o_{i_k} - a^o_{j_k} = 0$ and because $d(i_k j_k)$ divides b_{i_k}.

It remains to choose the remaining components of $\underline{a}^o$ so as to assure that $\underline{a}^o$ belongs to G_{k-1}. Let $A = \{Q_{i_k}, Q_{j_k}\}$. Then $\underline{a}^o$ R A; if $q = 0$, the relation holds vacuously, and if $q > 0$, it holds because f_k (or zero if $f_k = b_{i_k}$) is divisible by every d_r. In either case, according to Theorem 8 the remaining components of $\underline{a}^o$ can then be chosen so that $\underline{a}^o$ R B. This is a sufficient condition for $\underline{a}^o$ to belong to G_{k-1}, for the relation $\underline{a}^o$ R B, which imposes for every path C in H connecting points Q_i and Q_j of B the condition that $a^o_i \equiv a^o_j \bmod d(C)$, imposes the condition in particular for the $k - 1$ paths each consisting of a single link; and the conditions for these $k - 1$ paths specialize precisely to the $k - 1$ conditions $a^o_{i_p} \equiv a^o_{j_p} \bmod d(i_p j_p)$, $p = 1, 2, \ldots, k - 1$, assuring that $\underline{a}^o$ belongs to G_{k-1}. This completes the proof of Theorem 9.

SECTION 7

ILLUSTRATIVE COMPUTATION

We illustrate the application of Theorems 7 and 9 by evaluating

$$N((1;\ 2)(1;\ 4)(1;\ 5)(2;\ 3)(3;\ 4)(3;\ 5)(4;\ 5))$$

when $n = 5$. For $k = 1$, the linear graph H is the discrete graph with $k - 1 = 0$ links; then $f_1 = 1$, and, by (9), $h_1 = d(i_1j_1)/f_1 = d(12)$. For $k = 2$, H has $k - 1 = 1$ link Q_1Q_2, but no path connects $Q_{i_2} = Q_1$ and $Q_{j_2} = Q_4$; then $f_2 = 1$ and $h_2 = d(i_2j_2)/f_2 = d(14)$. For $k = 3$, H has $k - 1 = 2$ links Q_1Q_2 and Q_1Q_4, but no path connects $Q_{i_3} = Q_1$ and $Q_{j_3} = Q_5$; then $f_3 = 1$ and $h_3 = d(i_3j_3)/f_3 = d(15)$. For $k = 4$, H has $k - 1 = 3$ links Q_1Q_2, Q_1Q_4, Q_1Q_5, but no path connects $Q_{i_4} = Q_2$ and $Q_{j_4} = Q_3$; then $f_4 = 1$ and $h_4 = d(i_4j_4)/f_4 = d(23)$. For $k = 5$, H has $k - 1 = 4$ links Q_1Q_2, Q_1Q_4, Q_1Q_5, Q_2Q_3, and, in this graph, $Q_{i_5} = Q_3$ and $Q_{j_5} = Q_4$ are connected by the path $Q_3Q_2Q_1Q_4$; then $f_5 = d(3214)$, and, by (9), $h_5 = d(i_5j_5)/f_5 = d(34)/d(3214)$. For $k = 6$, H has the links already mentioned and the link Q_3Q_4; in this graph, $Q_{i_6} = Q_3$ and $Q_{j_6} = Q_5$ are connected by the paths $Q_3Q_2Q_1Q_5$ and $Q_3Q_4Q_1Q_5$; then

$$f_6 = \left[d(3215),\ d(3415)\right] \text{ and}$$

$$h_6 = d(i_6 j_6)/f_6 = d(35)/\left[d(3215),\ d(3415)\right].$$

For $k = 7$, H has the links already mentioned and the link Q_3Q_5; in this graph, $Q_{i_7} = Q_4$ and $Q_{j_7} = Q_5$ are connected by the paths $Q_4Q_1Q_5$, $Q_4Q_3Q_5$, $Q_4Q_1Q_2Q_3Q_5$, and $Q_4Q_3Q_2Q_1Q_5$; then

$$f_7 = \left[d(415),\ d(435),\ d(41235),\ d(43215)\right] \text{ and}$$

$$h_7 = d(i_7 j_7)/f_7 = d(45)/\left[d(415),\ d(435),\ d(41235),\ d(43215)\right].$$

The associative and commutative laws for the operations least common multiple and greatest common divisor, together with the identities

$$\left[p,\ q\right] = pq/(p,\ q),\ \left[p,\ pq\right] = pq,\ (p,\ pq) = p,$$

which hold for all positive integers p and q, permit the indices appearing to be brought into lexicographic order and the f_k to be simplified to a form in which only greatest common divisors appear. Thus, by the associative and commutative laws alone, $f_5 = d(1234)$. By these laws together with the identities,

$$f_6 = \left[d(1235),\ d(1345)\right]$$

$$= \frac{d(1235)d(1345)}{(d(1235),\ d(1345))} = \frac{d(1235)d(1345)}{d(12345)},$$

$$f_7 = \left[d(145),\ d(345),\ d(12345)\right] = \left[d(145),\ d(345)\right]$$

$$= \frac{d(145)d(345)}{(d(145),\ d(345))} = \frac{d(145)d(345)}{d(1345)}.$$

Having simplified the f_k as far as possible, we substitute the corresponding $h_k = d(i_k j_k)/f_k$ into (6), obtaining

$$N((1;\ 2)(1;\ 4)(1;\ 5)(2;\ 3)(3;\ 4)(3;\ 5)(4;\ 5))$$

$$= b_1b_2b_3b_4b_5 \frac{1}{d(12)} \frac{1}{d(14)} \frac{1}{d(15)} \frac{1}{d(23)} \cdot$$

$$\cdot \frac{d(1234)}{d(34)} \frac{d(1235)d(1345)}{d(12345)d(35)} \frac{d(145)d(345)}{d(1345)d(45)}$$

$$= b_1b_2b_3b_4b_5 \frac{d(145)d(345)d(1234)d(1235)}{d(12)d(14)d(15)d(23)d(34)d(35)d(45)d(12345)} \cdot$$

A check on the final expression is provided by noting that, like the set of specified interferences, it is invariant under transposition of symbols 1 and 3, and likewise under transposition of 4 and 5. A more tedious check would be to repeat the calculation, specifying the same interferences in a different order.

SECTION 8

EXPLICIT FORMULAS FOR $F_n(\underline{b})$

We exhibit expressions for $F_n(\underline{b})$, n = 1, 2, 3, 4. They are obtained by substitution in (5), with individual terms being evaluated as in Section 7.

$$F_1(\underline{b}) = b_1,$$

$$F_2(\underline{b}) = b_1 b_2 \{1 - 1/d(12)\} = b_1 b_2 - [b_1, b_2],$$

$$\begin{aligned} F_3(\underline{b}) = b_1 b_2 b_3 \Big\{ 1 &- \Big[\frac{1}{d(12)} + \frac{1}{d(13)} + \frac{1}{d(23)}\Big] \\ &+ \Big[\frac{1}{d(12)d(13)} + \frac{1}{d(12)d(23)} + \frac{1}{d(13)d(23)}\Big] \\ &- \frac{d(123)}{d(12)d(13)d(23)}\Big\}, \end{aligned}$$

$$\begin{aligned} F_4(\underline{b}) = b_1 b_2 b_3 b_4 \Big\{ 1 &- \Big[\frac{1}{d(12)} + \frac{1}{d(13)} + \frac{1}{d(14)} \\ &+ \frac{1}{d(23)} + \frac{1}{d(24)} + \frac{1}{d(34)}\Big] \\ &+ \Big[\frac{1}{d(12)d(13)} + \frac{1}{d(12)d(14)} + \frac{1}{d(12)d(23)} \\ &+ \frac{1}{d(12)d(24)} + \frac{1}{d(12)d(34)} + \frac{1}{d(13)d(14)} \\ &+ \frac{1}{d(13)d(23)} + \frac{1}{d(13)d(24)} + \frac{1}{d(13)d(34)} \\ &+ \frac{1}{d(14)d(23)} + \frac{1}{d(14)d(24)} + \frac{1}{d(14)d(34)} \\ &+ \frac{1}{d(23)d(24)} + \frac{1}{d(23)d(34)} + \frac{1}{d(24)d(34)}\Big] \\ &- \Big[\frac{1}{d(12)d(13)d(14)} + \frac{d(123)}{d(12)d(13)d(23)} \end{aligned}$$

$$+ \frac{1}{d(12)d(13)d(24)} + \frac{1}{d(12)d(13)d(34)}$$

$$+ \frac{1}{d(12)d(14)d(23)} + \frac{d(124)}{d(12)d(14)d(24)}$$

$$+ \frac{1}{d(12)d(14)d(34)} + \frac{1}{d(12)d(23)d(24)}$$

$$+ \frac{1}{d(12)d(23)d(34)} + \frac{1}{d(12)d(24)d(34)}$$

$$+ \frac{1}{d(13)d(14)d(23)} + \frac{1}{d(13)d(14)d(24)}$$

$$+ \frac{d(134)}{d(13)d(14)d(34)} + \frac{1}{d(13)d(23)d(24)}$$

$$+ \frac{1}{d(13)d(23)d(34)} + \frac{1}{d(13)d(24)d(34)}$$

$$+ \frac{1}{d(14)d(23)d(24)} + \frac{1}{d(14)d(23)d(34)}$$

$$+ \frac{1}{d(14)d(24)d(34)} + \frac{d(234)}{d(23)d(24)d(34)} \Bigg]$$

$$+ \Bigg[\frac{d(123)}{d(12)d(13)d(14)d(23)} + \frac{d(124)}{d(12)d(13)d(14)d(24)}$$

$$+ \frac{d(134)}{d(12)d(13)d(14)d(34)} + \frac{d(123)}{d(12)d(13)d(23)d(24)}$$

$$+ \frac{d(123)}{d(12)d(13)d(23)d(34)} + \frac{d(1234)}{d(12)d(13)d(24)d(34)}$$

$$+ \frac{d(124)}{d(12)d(14)d(23)d(24)} + \frac{d(1234)}{d(12)d(14)d(23)d(34)}$$

$$+ \frac{d(124)}{d(12)d(14)d(24)d(34)} + \frac{d(234)}{d(12)d(23)d(24)d(34)}$$

$$+ \frac{d(1234)}{d(13)d(14)d(23)d(24)} + \frac{d(134)}{d(13)d(14)d(23)d(34)}$$

$$+ \frac{d(134)}{d(13)d(14)d(24)d(34)} + \frac{d(234)}{d(13)d(23)d(24)d(34)}$$

$$+ \frac{d(234)}{d(14)d(23)d(24)d(34)} \Bigg]$$

$$- \Bigg[\frac{d(123)d(124)}{d(12)d(13)d(14)d(23)d(24)}$$

$$+ \frac{d(123)d(134)}{d(12)d(13)d(14)d(23)d(34)}$$

$$+ \frac{d(124)d(134)}{d(12)d(13)d(14)d(24)d(34)}$$

$$+ \frac{d(123)d(234)}{d(12)d(13)d(23)d(24)d(34)}$$

$$+ \frac{d(124)d(234)}{d(12)d(14)d(23)d(24)d(34)}$$

$$+ \frac{d(134)d(234)}{d(13)d(14)d(23)d(24)d(34)}\Bigg]$$

$$+ \frac{d(123)d(124)d(134)d(234)}{d(12)d(13)d(14)d(23)d(24)d(34)d(1234)}\Bigg\}.$$

SECTION 9

NUMERICAL EXAMPLE

The formulas of the preceding section may be made even more concrete by substituting specific numerical values. Thus, let $n = 3$, $b_1 = 6$, $b_2 = 10$, $b_3 = 15$. Then $d(12) = 2$, $d(13) = 3$, $d(23) = 5$, $d(123) = 1$,

$$\begin{aligned} F_3(\{6,\ 10,\ 15\}) &= 6\cdot10\cdot15\Big\{1 - \Big[\frac{1}{2} + \frac{1}{3} + \frac{1}{5}\Big] \\ &\qquad + \Big[\frac{1}{2\cdot3} + \frac{1}{2\cdot5} + \frac{1}{3\cdot5}\Big] - \frac{1}{2\cdot3\cdot5}\Big\} \\ &= 900\{(30 - 15 - 10 - 6 + 5 + 3 + 2 - 1)/30\} \\ &= 30\cdot8 = 240. \end{aligned}$$

It can be proved by induction on n that the subgroup, say J, of G_0 consisting of those members of G_0 which exhibit all possible interferences is the cyclic subgroup of order $[b_1, b_2, \ldots, b_n]$ generated by $\{1, 1, \ldots, 1\}$. Clearly two members of a coset relative to J exhibit precisely the same interferences. In the present numerical example, the subset T of G_0 whose members exhibit no interferences is the union of eight such cosets. The following list shows one representative from each of these eight cosets:

$$\{0, 1, 2\},\ \{0, 1, 4\},\ \{0, 1, 5\},\ \{0, 1, 7\},$$
$$\{0, 1, 8\},\ \{0, 1, 10\},\ \{0, 1, 13\},\ \{0, 1, 14\}.$$

The full set T, with 240 members, is then obtained by adding multiples of $\{1, 1, 1\}$ to these eight triples.

SECTION 10

A REDUCTION PRINCIPLE

Since there are $2^{n(n-1)/2}$ terms in the general formula (5) for $F_n(\underline{b})$, and since the individual terms become more complicated as n increases, evaluation of $F_n(\underline{b})$ by direct substitution in (5) soon becomes prohibitively tedious. In some cases the following reduction principle permits an abbreviated calculation.

Theorem 10 (Reduction principle). If $F_m(\{b_{i_1}, b_{i_2}, \ldots , b_{i_m}\}) = 0$, where $\{i_1, i_2, \ldots , i_m\}$ is an m-tuple of distinct positive integers none of which exceeds n, then $F_n(\underline{b}) = 0$.

Proof: The hypothesis implies that each $\underline{a}$ in G_o exhibits at least one of the $m(m - 1)/2$ interferences $(i_1; i_2), (i_1; i_3), \ldots , (i_{m-1}; i_m)$. Then each $\underline{a}$ in G_o exhibits at least one interference chosen from the full set of $n(n - 1)/2$ interferences, so that $F_n(\underline{b}) = 0$, q. e. d.

Theorem 11. If $d(ij) = 1$ for some pair $\{i, j\}$, $i \neq j$, then $F_n(\underline{b}) = 0$.

Proof: If $d(ij) = 1$, then, according to Section 8, $F_2(\{b_i, b_j\}) = 0$. Then $F_n(\underline{b}) = 0$ by Theorem 10.

Theorem 12. If $b_1 = b_2 = \dots = b_n = b$, say, then

(10) $F_n(\underline{b}) = b(b - 1)(b - 2) \dots (b - n + 1)$.

Proof: a_1 can be chosen in b ways. This choice made, a_2 can be chosen in $b - 1$ ways to avoid interference, and so on. If $b \geq n$, the process can be continued until finally a_n can be chosen in $b - n + 1$ ways. Thus, (10) is correct if $b \geq n$. If $b < n$, however, there exists no $(b + 1)$-tuple $\{a_1, a_2, \dots , a_{b+1}\}$ of distinct integers all satisfying $0 \leq a_i < b$. Then $F_{b+1}(\{b_1, b_2, \dots , b_{b+1}\}) = 0$, so, by Theorem 10, $F_n(\underline{b}) = 0$. On the other hand, if $b < n$, one of the factors on the right-hand side of (10) is zero, so that (10) yields the correct result.

REFERENCES

1. Dickson, L. E. History of the Theory of Numbers. Vol. II. New York: Chelsea Publishing Company, 1952.

2. Ledermann, W. Introduction to the Theory of Finite Groups. Third ed. Edinburgh: Oliver and Boyd, Ltd., 1957.

3. Riordan, J. An Introduction to Combinatorial Analysis. New York: John Wiley & Sons, Inc., 1958.

BIOGRAPHICAL SKETCH

Edward Allen Fay was born August 13, 1918, at Berkeley, California. Educated in the Berkeley public schools, he was graduated from Berkeley High School in 1935. He received the degree Bachelor of Arts, with highest honors in mathematics, from the University of California in 1939, and the degree Master of Arts in mathematics from Harvard University in 1941. During the academic year 1941-1942 he was a teaching assistant in mathematics at the University of Rochester, Rochester, New York, and from 1942 to 1943 he was employed as an inspector of ordnance material by the Rochester Ordnance District. From 1943 to 1946 he was a member of the United States Army, serving in the United States, France, and Germany.

Returning to Berkeley after the war, Mr. Fay was a teaching assistant in mathematics at the University of California during the 1946 summer session, and a graduate student in mathematical statistics from 1946 to 1950. Since 1950 he has been employed as a mathematical statistician at the United States Naval Ordnance Test Station, China Lake, California. Since June, 1961, he has been a graduate student in mathematics at the University of Florida under an educational fellowship from the United States Naval Ordnance Test Station.

Edward Allen Fay is married to the former Dorothy Louise Tevis and is the father of three children. His interests within the field of mathematical statistics include combinatorial theory, stochastic processes, and techniques of sampling inspection. He is a member of the American Mathematical Society, the Mathematical Association of America, the Institute of Mathematical Statistics, the Association for Symbolic Logic, the Scientific Research Society of America, and Phi Beta Kappa. He is a lay reader in the Episcopal church.

This dissertation was prepared under the direction of the chairman of the candidate's supervisory committee and has been approved by all members of that committee. It was submitted to the Dean of the College of Arts and Sciences and to the Graduate Council, and was approved as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

June 11, 1962

Dean, College of Arts and Sciences

Dean, Graduate School

Supervisory Committee:

Chairman

R. G. Blake

E. H. Hadley

Willard